ThreatConnect.

Customer Spotlight

Large Healthcare Services and Technology Enterprise Streamlines Threat Intelligence Operations

Customer Profile

Org. Size	*Industry/Sector*	*Headquarters*
>300,000 EMPLOYEES	HEALTHCARE TECH AND SERVICES	U.S. BASED

Background

As one of the world's largest healthcare services and technology enterprises, this organization supports clinical, administrative, and digital operations across thousands of sites and millions of patients. With such scale and complexity, maintaining a proactive and high-fidelity threat intelligence program is essential to protecting sensitive healthcare data and ensuring uninterrupted care delivery.

The organization faces a high volume of ransomware, credential-theft, third-party compromise, and healthcare-specific threat activity, including attacks against clinical systems, patient portals, and billing platforms. Intelligence needed to be actionable at the speed of security operations — not just stored. Despite strong security investments, the company's threat intelligence workflows were fragmented and difficult to scale. To better support detection engineering, incident response, and cross-team decision-making, their Cyber Threat Intelligence (CTI) program leveraged ThreatConnect TI Ops — unifying data, improving context, and enabling faster, more informed security decisions across teams.

Challenges Faced

Before adopting ThreatConnect, the enterprise relied on an open source Threat Intelligence Platform, several standalone threat feeds, and manual workflows largely maintained by a single analyst. While these tools provided raw intelligence, the data was not unified, enriched, or actionable. Integrations with SIEMs, SOARs, EDRs, and other operational systems were limited, slowing down investigations and reducing the effectiveness of downstream security tools. The team also struggled to scale intelligence operations as threat volume and business complexity increased. Key challenges included:

- Difficulty integrating with operational tools (SIEM, SOAR, EDR, XDR)
- Inefficient and time-intensive threat intelligence workflows
- Limited context around threats and indicators
- Lack of scalability and flexibility in CTI operations
- Fragmented data stored across disparate tools, feeds, and repositories

> "We were using an open source solution, managed by one person, and several threat feeds, but the data was not in a format or platform that allowed us to use it properly. We just weren't as effective. We needed a platform that would allow us to aggregate our threat data and manipulate it for actionable intelligence."
>
> **— Sr. Cybersecurity Analyst, Large Healthcare Services and Technology Company**

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

How ThreatConnect Helped

The organization selected ThreatConnect Threat Intelligence Platform (TI Ops) based on its strong consultative partnership, pricing value, integration capabilities, and overall product functionality. ThreatConnect's alignment with CTI tradecraft — including intelligence requirements, automation capabilities, and deep customization — provided the flexibility and structure needed to modernize the program. With TI Ops, the team can now centralize all threat data, enrich it automatically, and distribute high-fidelity intelligence into operational tools across the SOC. Features such as the ATT&CK Visualizer, integrations, Threat Graph, automation, and developer-friendly APIs have driven significant improvements in speed, quality, and consistency.

Results achieved:

- High performance and scalability across millions of IOCs
- Ability to operationalize threat intelligence across detection, IR, and defense
- Alignment with CTI tradecraft, including intelligence requirements
- Flexible customization of workflows, data models, and playbooks
- Strong contextualization of threats with automated enrichments
- Access to additional high-value threat feeds

"ThreatConnect has allowed us to improve the quality of CTI output, which feeds the rest of Security Operations and the Defense team. We are able to more efficiently improve detections, improve incident response through more informed research through ThreatConnect, and better testing using the intelligence provided through ThreatConnect."
— Sr. Cybersecurity Analyst, Large Healthcare Services and Technology Company

Unifying Threat, Risk, and Action Across Teams

ThreatConnect has transformed how the organization produces, shares, and applies threat intelligence. By consolidating all threat data and reporting into one platform, teams across the SOC, IR, and threat hunting functions are now operating from a single, consistent source of truth. This alignment has improved communication, accelerated investigations, and increased the effectiveness of other security tools — enabling a more proactive, intelligence-driven approach to defense.

Results achieved:

- Reduced false positive rate by 50–75%
- Reduced MTTR for standard incidents
- Somewhat reduced workload across the team through automation
- Improved effectiveness of SIEM, EDR, XDR, SOAR, and other tools
- Stronger cross-team alignment with unified reporting and data sources
- Critical platform for day-to-day operations

About ThreatConnect:

ThreatConnect powers smarter, faster, and more resilient cyber defense by uniting threat intelligence, security operations, and cyber risk management. Our Intel Hub platform brings threat and risk data together to help organizations prioritize what matters most, operationalize defenses more efficiently, and communicate cyber risk in business terms. Trusted by over 250 global enterprises, ThreatConnect enables security teams to adapt to evolving threats, make better decisions, and prove their impact — from the SOC to the C-suite.

ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240